DETEKSI INDIKASI FRAUD DENGAN TEKNOLOGI AUDIT

Fitri Annisa[1], Lutfi Harris[2]
[1] *Jurusan Akuntansi, Fakultas Ekonomi, Universitas Brawijaya*
Jl. MT Haryono 165 Malang 65145
Telp (0354)567040 Fax (0354)567040
[2] *Jurusan Akuntansi, Fakultas Ekonomi, Universitas Brawijaya*
Jl. MT Haryono 165 Malang 65145
Telp (0354)567040 Fax (0354)567040
E-mail: fitri.annisa.2006@gmail.com, lutfi@smart.co.id

ABSTRAK
The aim of this research is describing how to detect fraud using Computer Assisted Audit Technique (TABK). This research focus on purchasing fraud. Qualitative research method has used in this research.Symptoms of fraud can be separated into six categories: accounting anomalies, internal control weaknesses, analytical anomalies, extravagant lifestyle, unusual behavior, and tips and complaint. Auditor can use TABK especially to detect accounting anomalies, and analytical anomalies. The using TABK in detecting fraud can increase the effectiveness and efficiency of audit process. In the company which was implementing computer based information system, most of the data was stored in digital format, it could not read directly, and only a little physical audit tracking. Therefore, this is the chance for the auditor to use TABK to detect symptoms of fraud. When the auditor find fraud's symptoms, he or she must investigate whether the symptoms resulted from actual fraud or by other factors. The result of the test using TABK is just a mediator for the auditor to find fraud's symptoms. So, the auditors have to do further investigation. By using TABK, the process to detect fraud will be able to be done more effective and efficient.

Keywords : Fraud, Purchasing fraud, Fraud Symptoms, Computer Assisted Audit Technique(TABK)

1. LATAR BELAKANG

Salah satu dampak perkembangan teknologi yang nyata dalam praktik bisnis adalah pemrosesan data yang awalnya manual, sekarang dilakukan terkomputerisasi. Sebagian besar perusahan menengah besar telah menggunakan *software* akuntansi dalam pencatatan dan pelaporan keuangannya. Penggunaan *software* akuntansi ini menyebabkan beberapa proses akuntansi manual sudah mulai ditinggalkan. Selain manfaat ekonomi yang diperoleh, muncul risiko baru yang dihadapi oleh pebisnis yaitu munculnya tindakan kejahatan *(fraud)* dengan memanfaatkan teknologi komputer. Risiko fraud ini menjadi satu faktor yang harus disadari oleh profesi akuntan khususnya dalam rangka pelaksanaan audit laporan keuangan.

Auditor memiliki peran penting untuk menemukan indikasi adanya tindakan fraud dalam penyajian laporan keuangan *auditee*. Sesuai Standar Audit seksi 327, dalam lingkungan sistem informasi akuntansi terkomputerisasi, maka tidaklah praktis bagi auditor untuk melakukan pengujian manual. Karena itulah, teknik audit terkomputerisasi dan *aplikasi* audit akan banyak membantu auditor untuk lebih fokus terhadap area yang beresiko tinggi.

Dalam upaya meningkatkan efektifitas dan efisiensi proses pendeteksian *fraud,* auditor seyogyanya mempertimbangkan penggunaan teknik – teknik audit berbasis komputer yang dikenal dengan istilah Teknik Audit Berbantuan Komputer (TABK) (SA 327). Terdapat bermacam – macam jenis tindakan *fraud* dalam aktifitas bisnis. ACFE memetakan 51 jenis *fraud* yang terbagi dalam tiga jenis, yaitu *Corruption, Fraudulent Statements,* serta *Asset Misappropriation* (Tuanakotta, 2007:96).

Dalam mendeteksi *Asset Misappropriation,* penggunaan TABK dapat dikelompokkan dalam beberapa area fungsional, antara lain area pembelian, area penjualan, serta area penggajian (Hunton, 2006:201). Salah satu fungsi yang rawan beresiko *fraud* adalah bagian pembelian *(purchasing)*. Area pembelian cenderung menanggung resiko kecurangan yang tinggi untuk *misappropriation (*Coderre 2009:185). Kecurangan di area tersebut sering melibatkan kolusi antara karyawan dengan pihak ketiga. *Fraud* yang umumnya terjadi di dalam *purchasing area* antara lain pembayaran kepada vendor fiktif, serta pembayaran atas barang yang tidak pernah diterima. *Fraud* tersebut dapat dilakukan oleh *employee*, *vendor*, maupun kerjasama antara *vendor* dan *employee*. Lemahnya pengendalian internal, merupakan salah satu peluang yang memicu terjadinya *fraud* di area tersebut.

Berdasar latar belakang ini, penulis memfokuskan penelitian tentang penerapan Teknik Audit Berbantuan Komputer (TABK) dalam mendeteksi kemungkinan terjadinya *fraud* pada *purchasing area,* di mana peluang yang memicu

terjadinya *fraud* di area tersebut salah satunya disebabkan oleh lemahnya pengendalian internal perusahaan.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif deskriptif. Alasan penulis menggunakan metode kualitatif adalah untuk mendapatkan data / informasi yang lebih lengkap, mendalam, kredibel dan bermakna, sehingga tujuan penelitian dapat dicapai. Penelitian ini menggunakan jenis data sekunder, artikel, buku maupun jurnal serta literatur lain yang mendukung.

Sumber data dalam penelitian ini berasal dari literatur seperti buku, jurnal penelitian, makalah, serta beberapa artikel terkait. Hasil kajian pemikiran yang tertuang dalam berbagai literatur menjadi landasan dalam proses telaah secara mendalam atas penerapan TABK dalam mendeteksi kemungkinan terjadinya *fraud*.

Analisis dan interpretasi hasil penelitian ini dilakukan dengan menggali persoalan potensial penerapan TABK dalam mendeteksi kemungkinan terjadinya *fraud*.

3. PEMBAHASAN

3.1 Purchasing Fraud

Salah satu fungsi yang rawan beresiko *fraud* adalah bagian pembelian *(purchasing). Fraud* di bagian tersebut hampir terjadi di semua organisasi, dan menempati tingkat yang tinggi dalam aktivitas kecurangan (Coderre, 2009:173). *Fraud* di area pembelian umumnya berupa *invoice scheme, kick back, fix bidding*.

a. Invoice Scheme

Dalam *invoice scheme*, faktur yang dicurangi *(fraudulent invoice)* dikirimkan ke perusahaan, baik oleh karyawan perusahaan, maupun pihak ketiga. Kebanyakan dari skema permainan tersebut, perusahaan membuat vendor fiktif, dan kemudian mengirimkan faktur fiktif kepada perusahaan untuk dilunasi (Frank, dalam Golden *et al*, 2006:236).

Secara implisit, Davia (2005:72) menyebutkan *invoice scheme* sebagai *elementary fraud type*. *Fraud* ini banyak dijumpai di berbagai perusahaan karena relatif sederhana dan mudah dilakukan. *Elementary fraud type* terdiri dari *duplicate payment fraud, multiple payee fraud,* serta *shell fraud.*

Duplicate payment fraud meliputi penerbitan dua atau lebih check yang serupa untuk membayar tagihan yang sama. *Fraud* akan terjadi ketika karyawan yang memiliki niat jahat mengajukan dokumen yang diperlukan untuk menyebabkan pembayaran ganda dalam melunasi tagihan dari kreditor. Satu check digunakan untuk membayar vendor sebenarnya *(real vendor),* dan check yang lain dicuri oleh pelaku (Davia, 2005:72).

Multiple payee fraud meliputi dua atau lebih pembayaran kepada *payee* yang berbeda untuk item barang yang sama. Salah satu pembayaran ditujukan kepada kreditor yang sah, dan pembayaran lain ditujukan kepada pelaku (Davia, 2005:76).

Shell fraud, disebut shell fraud karena barang yang dibeli dan dibayar tidak ada dan tidak akan pernah ada. Dasar dari pembayaran *shell fraud* seluruhnya fiktif (Davia, 2005:80). Karyawan membuat perusahaan fiktif dan kemudian mengirim faktur fiktif dari vendor fiktif kepada perusahaan untuk dibayarkan. Di sini, pelaku harus memiliki kemampuan untuk menambahkan vendor ke dalam daftar vendor yang telah disetujui, menyetujui faktur dari vendor, atau untuk memperoleh persetujuan atas tagihan dari vendor (Frank, dalam Golden *et al*, 2005:2*37).*

b. Kickbacks

Coderre (2009:187) mengungkapkan *kickbacks* terjadi ketika *vendor* melakukan pembayaran secara ilegal kepada karyawan yang melakukan aktivitas pembelian dalam menjalankan bisnisnya. Pembayaran tersebut dilakukan agar karyawan di bagian pembelian melakukan beberapa aktivitas berikut :

1. Memberikan kontrak pembelian hanya kepada *vendor* tertentu.
2. Membuat tanda terima barang atas barang yang sebenarnya tidak diterima.
3. Menyetujui pembayaran atas faktur ganda.
4. Menyutujui penerimaan barang yang berkualitas lebih rendah daripada barang yang dipesan.
5. Memberikan syarat pembayaran *(credit term)* yang menguntungkan *vendor.*
6. Membayar barang dengan harga yang lebih tinggi.
7. Membayar tagihan / utang lebih awal tanpa mendapatkan diskon pembelian.
8. Membeli barang dengan jumlah yang lebih banyak dari yang dibutuhkan.

c. Fixed Bidding

ACFE menyebutkan bahwa *bid rigging* adalah pengaturan hasil tender secara ilegaloleh karyawan yang terkait dengan bagian pembelian untuk memenangkan *vendor* tertentu. Sementara itu, Coderre (2009:190) menyebut istilah *bid rigging* dengan *fixed bidding*, yang meliputi beberapa aktivitas yang dilakukan untuk memperlakukan salah satu kontraktor lebih baik daripada kontraktor lainnya. Beberapa aktivitas yang dimaksud Coderre meliputi hal – hal sebagai berikut :

1. Terdapat vendor yang memenangkan kontrak tanpa melalui proses tender yang resmi.

2. Terdapat kontrak yang dilakukan dengan penunjukan langsung, tanpa dasar alasan yang jelas.
3. Memecah nilai kontrak *(spliting contract)* untuk menghindari *financial limits*, sehingga vendor akan memenangkan tender.
4. Menjamin salah satu vendor agar sering memenangkan tender.
5. Mengatur agar vendor yang memasukkan penawaran mendekati tanggal pengumuman, secara konsisten memenangkan tender.

Di Indonesia, ketentuan penyelenggaraan tender diatur dalam Keputusan Presiden No. 80 tahun 2003 tentang Pedoman Pelaksanaan Pengadaan Barang / Jasa Pemerintah (Pedoman Pengadaan Barang / Jasa). Ketentuan Keppres tersebut berlaku khusus untuk pengadaan barang / jasa Pemerintah yang dibiayai Anggaran Pendapatan dan Belanja Negara (APBN) / Anggaran Pendapatan dan Belanja Daerah (APBD) (Harjono:2007).

Terdapat banyak kasus penyelenggaraan tender yang diadukan kepada Komisi Pengawas Persaingan Usaha (KPPU) atau bahkan diadukan kepada pihak Kepolisian. Pengaduan tersebut umumnya berdasarkan kepada adanya penunjukan langsung atau proses tender lainnya yang tidak sesuai dengan ketentuan yang berlaku, apalagi bila salah satu peserta tender dimenangkan *(fix bidding)* tanpa alasan yang jelas.

Praktik persekongkolan dalam tender ini dilarang karena dapat menimbulkan persaingan tidak sehat dan bertentangan dengan tujuan dilaksanakannya tender untuk memberikan kesempatan yang sama kepada pelaku usaha agar dapat ikut menawarkan harga dan kualitas yang bersaing. Sehingga pada akhirnya dalam pelaksanaan proses tender tersebut akan didapatkan harga yang termurah dengan kualitas yang terbaik (KPPU, 2009).

3.2 Penggunaan TABK Dalam Mendeteksi Fraud

Salah satu prosedur yang dilakukan dalam mendeteksi *fraud* adalah memeriksa ketersediaan data untuk mengindentifikasikan gejala *fraud*. Karena auditor tidak mungkin menguji secara manual setiap transaksi yang terjadi, maka penerapan prosedur audit mungkin mengharuskan auditor untuk mempertimbangkan teknik audit berbantuan komputer (TABK).

Albrecht (2006) menggolongkan TABK sebagai pendekatan proaktif dalam upaya pendeteksian *fraud*. TABK dapat digunakan untuk memeriksa data dengan ukuran yang besar dalam rangka menemukan suatu anomali yang mungkin menunjukkan gejala *fraud*, misalnya *inaccuracies in ledgers*, yaitu adanya ketidaksesuaian antara jumlah yang terdapat dalam buku besar dengan jumlah yang terdapat dalam buku pembantunya.

Pendekatan proaktif dalam mendeteksi *fraud* menggunakan *software* untuk mencari anomali dalam *data base*. *Software* yang umum digunakan antara lain adalah *Audit Command Language (ACL)*, CaseWare IDEA, Microsoft Excel, Monarch, dan sebagainya. Keuntungan utama dari penggunaan *software* tersebut adalah mudah digunakan, serta dapat memeriksa keseluruhan transaksi dalam ukuran yang besar, sehingga pendeteksian *fraud* dapat dilakukan secara efektif dan efisien.

Pemanfaatan software audit akan sangat membantu auditor dalam pelaksanaan tugasnya. Auditor dapat merancang kertas kerja *(working paper)* dengan bantuan *software* audit. Tidak jarang auditor harus melakukan prosedur audit lanjutan dengan mengubah pertanyaan *(queries)* yang diajukannya. Karena itu, software audit mendokumentasikan seluruh langkah ini dalam *command log*.

3.3 Mendeteksi Fraud di Area Pembelian Dengan Menggunakan TABK

Untuk mendeteksi *fraud*, seorang auditor harus mengenali indikasi terjadinya *fraud(symptom)* dan memeriksa apakah gejala tersebut berasal dari *fraud* yang sebenarnya atau disebabkan oleh faktor lain. Banyak *fraud* yang akan dideteksi lebih cepat jika auditor mengenali gejala *fraud* yang terjadi. Akan tetapi, perlu dilakukan pemeriksaan lebih lanjut untuk melihat apakah gejala tersebut berasal dari *fraud* yang sebenarnya.

Seperti yang dijelaskan sebelumnya, terdapat 3 jenis *fraud* yang terjadi di area pembelian, yaitu *invoice scheme,kick back*, dan *fixed bidding*. Jika seorang auditor ingin mendeteksi *fraud* di area pembelian, maka ia harus mengenali indikasi terjadinya *fraud(symptom)* di area tersebut. Bagian berikut ini akan menjelaskan gejala *fraud* yang terjadi di area pembelian beserta cara mendeteksinya menggunakan TABK.

a. Mengenali gejala *invoice scheme*

Dalam *invoice scheme*, faktur yang dicurangi *(fraudulent invoice)* dikirimkan ke perusahaan, baik oleh karyawan perusahaan, maupun pihak ketiga (Frank dalam Golden *et al*, 2006:236). Secara implisit, Davia (2005:72) menyebutkan *invoice scheme* sebagai *elementary fraud type* yang terdiri dari *duplicate payment fraud, multiple payee fraud,* serta *shell fraud.*

Berikut adalah beberapa gejala *fraud* yang termasuk dalam kelompok *Invoice scheme :*

1. faktur yang difotokopi (Coderre, 2009:188).
2. vendor yang memiliki alamat yang sama dengan karyawan (Coderre, 2009:188).
3. vendor yang memiliki alamat P.O. BOX (Clayton dalam Golden et al, 2006:410; Coderre, 2009:188; Elrington, tanpatahun; Warner, tanpa tahun).

4. vendor dengan nama seperti "Mr.," "Mrs.," atau nama lain yang dengan mudah bias dirubah untuk membuat agar pembayaran dapat dilakukan kepada seseorang (Coderre, 2009:189).
5. nama vendor yang sama dalam database vendor (Clayton dalam Golden et al, 2006:410).
6. Terdapat 2 atau lebih vendor yang berbeda, tetapi memiliki alamat yang sama (Clayton dalam Golden et al, 2006:410).
7. Terdapat *sequential vendor invoice number*. (Coderre, 2009:189 ; Frank dalam Golden et al, 2006:237 ; Elrington, tanpa tahun).
8. Terdapat banyak transaksi yang berada sedikit di bawah *financial treshold.* Coderre (2009:188)

Faktur yang difotokopi (nomor 1) mengindikasikan terjadinya *duplicate payment fraud.* Sementara itu, gejala yang terkait dengan vendor yang dianggap mencurigakan *(nomor 2 – 7)* mengindikasikan terjadinya *multiple payee fraud* dan *shell fraud* yang berkaitan dengan pembayaran kepada vendor fiktif.

Tahapan pengujian untuk mendeteksi adanya fraud dengan aplikasi audit ACL adalah sebagai berikut:

1. Mengidentifikasi file transaksi pembelian, vendor master file, serta employee master file.
2. Permintaan data kepada klien.
3. Melakukan importing data ke dalam ACL
4. Melakukan verifikasi atas integritas data.
5. Melakukan pengujian spesifik menggunakan CAAT untuk menemukan duplicate payment fraud. Periksalah apakah terdapat duplikat pada nomor faktur dengan menggunakan fungsi look for duplicate yang terdapat dalam menu ACL
9. Melakukan pengujian spesifik menggunakan fungsi *joint table* CAAT untuk mencari vendor fiktif atau vendor yang diangap mencurigakan *(suspicious vendor).*
10. Mencari nama vendor yang sama dengan menggunakan perintah *look for duplicate* pada field nama dan field alamat dalam vendor master file.
11. Mencari *sequential vendor invoice number* dengan cara melakukan *classify* pada nomor dan nama vendor yang terdapat dalam tabel transaksi pembelian.
12. Memeriksa apakah terdapat nilai kontrak atau nilai dari faktur yang dipecah untuk menghindari *financial limit* dengan menggunakan analisis Benford.

b. Mengenali gejala *kickback*

Seperti yang dijelaskan sebelumnya, *kickback* dilakukan oleh vendor agar karyawan di bagian pembelian melakukan beberapa aktivitas seperti menyetujui penerimaan barang yang berkualitas lebih rendah daripada barang yang dipesan, membayar barang dengan harga yang lebih tinggi, membeli barang dengan jumlah yang lebih banyak dari yang dibutuhkan, dan sebagainya (Coderre, 2009:189). Sehingga jika terdapat beberapa aktivitas tersebut, auditor perlu mencurigai apakah aktivitas tersebut dipicu oleh *kickback.*

Berikut adalah beberapa gejala adanya *kickback*:

1. Perusahaan melakukan pemesanan barang tertentu, padahal jumlah barang yang tersedia *(quantity on hand)* jauh lebih besar di atas titik pemesanan barang *(re ordered point).*
2. Terdapat vendor tertentu yang mendominasi pembelian secara tidak wajar.
3. Jumlah barang yang diterima tidak sama dengan jumlah barang yang dipesan.
4. Terdapat vendor tertentu yang sering mengirimkan barang dengan kualitas yang lebih rendah.
5. Terdapat pembelian barang dengan harga yang lebih mahal daripada yang dibutuhkan, dan tanpa didasari alasan yang jelas.

Tahapan pengujian yang dapat dilakukan untuk mendeteksi adanya indikasi *kickback* dengan aplikasi ACL adalah sebagai berikut:

1. Mengidentifikasi *file* yang diperlukan dalam pengujian *kick back* antara lain *file inventory* dan *file* transaksi pembelian.
2. Permintaan data kepada klien
3. Melakukan *importing data file inventory* dan *file* transaksi pembelian ke dalam ACL.
4. Melakukan *verifikasi atas integritas data.*
5. Melakukan pengujian spesifik menggunakan *CAAT* untuk menemukan apakah terdapat pemesanan barang yang dilakukan jauh sebelum barang mencapai *re order point.*
6. Mencocokkan jumlah barang yang dipesan dengan jumlah barang yang diterima dengan fungsi *Join.*
7. Memeriksa apakah terdapat penerimaan barang yang berkualitas lebih rendah dari barang yang dipesan, dengan fungsi *summarize.*
8. Memeriksa apakah terdapat pembelian barang dengan harga yang lebih mahal daripada yang dibutuhkan dengan fungsi *summarize.*

Dari hasil pengujian ini, bila terdapat kecenderungan pemesanan barang padahal *quantity on hand* masih aman, terdapat vendor yang mendominasi supply barang secara intensif, dan terdapat kemungkinan adanya *mark up*, maka hal-hal tersebut mengindikasikan adanya *kickback.*

c. Mengenali gejala *Fix bidding*

Menurut Coderre (2009:190), aktivitas yang menunjukkan gejala fix bidding antara lain sebagai berikut :

1. Terdapat vendor yang memenangkan kontrak tanpa melalui proses tender yang resmi.

2. Terdapat kontrak yang dilakukan dengan penunjukan langsung, tanpa dasar alasan yang cukup.
3. Memecah nilai kontrak *(spliting contract)* untuk menghindari *financial limits*, sehingga vendor akan memenangkan tender.
4. Menjamin salah satu vendor agar sering memenangkan tender.
5. Mengatur agar vendor yang memasukkan penawaran mendekati tanggal pengumuman, secara konsisten memenangkan tender.

Dalam upaya pencarian fix bidding, auditor perlu mempersiapkan prosedur audit yang menggunakan TABK sebagai berikut :

1. Mengidentifikasi file yang diperlukan dalam pengujian fix bidding antara lain file yang berisi informasi mengenai tender perusahaan.
2. Permintaan data kepada klien
3. Melakukan importing data ke dalam ACL.
4. Melakukan verifikasi atas integritas data
5. Melakukan pengujian spesifik menggunakan CAAT untuk menemukan fix bidding. Periksa tipe kontrak menggunakan perintah *summarize* untuk melihat apakah terdapat vendor yang memenangkan kontrak tanpa melalui proses tender yang resmi.
6. Memeriksa tanggal kontrak vendor untuk menemukan duplikat, dimana total nilai kontrak berada di atas *financial limit*, untuk melihat apakah terdapat vendor yang memenangkan tender dengan cara memecah nilai kontrak *(spliting contract)* untuk menghindari *financial limits.*
7. Melakukan *summarizing* pada field vendor untuk melihat apakah terdapat vendor yang paling sering memenangkan tender selama beberapa periode.
8. Membandingkan tanggal penerimaan dokumen penawaran dengan tanggal pengumuman hasil pemenang untuk melihat apakah terdapat vendor yang secara konsisten memenangkan tender dengan memasukkan penawaran mendekati tanggal pengumuman hasil tender. Fungsi filter perlu diatur sebagai berikut : award date – bid received date <= 2.

Dari hasil pengujian tersebut jika didapati vendor yang secara konsisten memenangkan tender dengan memasukkan penawaran mendekati tanggal pengumuman hasil tender, hal ini mengindikasikan bahwa ia mungkin mendapatkan informasi dari karyawan perusahaan semisal memperoleh informasi internal mengenai harga penawaran dari vendor lain (Elrington, tanpa tahun; Coderre, 2009:190)..

4. KESIMPULAN

Fraud dapat terjadi di berbagai fungsi organisasi. Salah satu fungsi yang rawan beresiko *fraud* adalah bagian pembelian *(purchasing). Fraud* di bagian tersebut hampir terjadi di semua organisasi, dan menempati tingkat yang tinggi dalam aktivitas kecurangan (Coderre, 2009:173). *Fraud* di area pembelian umumnya berupa *invoice scheme, kick back, fix bidding*.

Salah satu cara yang dapat dilakukan auditor dalam mendeteksi ada tidaknya fraud adalah dengan menggunakan Teknik Audit Berbantuan Komputer (TABK). Penggunaan TABK harus mempertimbangkan ketersediaan fasilitas komputer, sistem akuntansi, serta *database* dari klien. Jika ketiga hal tersebut tidak tersedia, maka penggunaan TABK tidak akan memberikan hasil yang efektif. Karena itulah, langkah – langkah penerapan TABK untuk mendeteki *fraud* bisa diaplikasikan pada perusahaan atau organisasi yang menggunakan sistem informasi akuntansi berbasis komputer.

Di samping menggunakan TABK, prosedur audit manual juga masih diperlukan. Hasil pengujian dari TABK hanya bersifat sebagai jembatan bagi auditor untuk menemukan gejala fraud dan melakukan investigasi lebih lanjut atas temuan yang didapat. Sehingga pendekatan audit dalam lingkungan yang terkomputerisasi hendaknya mempertimbangkan suatu kombinasi antara teknik audit secara manual dan teknik audit berbantuan komputer

PUSTAKA

Albrecht, W. Steve., Albrecht, Conan C., Albrecht Chad O. (2006). *Fraud Examination*. Canada : South - Western, a division of Thomson Learning.

Association of Certified Fraud Examiners (ACFE). (2008). *ACFE Report to The Nations 2008*

Coderre, David. (2009). *Computer-Aided Fraud Prevention and Detection*. Hoboken, New Jersey : John Wiley & Sons, Inc.

Davia, Howard. (2005). *Fraud 101 Techniques and Strategies for Detection*. Hoboken, New Jersey : John Wiley & Sons, Inc.

Elrington, Sean. (Tanpa tahun). *Fraud Test using Audit Tools*. http://www.ziddu.com /download/ 3564632/ 1_022508_ frauddemo.zip.html (Diakses pada 15 September 2009).

Golden, T.W., Skalak, Steven L., Clayton, Mona M. (2006). *A Guide to Forensic Accounting Investigation*. Hoboken, New Jersey : John Wiley & Sons, Inc.

Harjono, Dhaniswara K. (2007). Hukum – Bagaimana Penyelenggaraan Sebuah Tender. http://www.majalahpengusaha.com/content/view/282/133 (Diaksespada 30 Maret 2009)

Hunton, J.E., Bryant, Stephanie M., Bagranoff, Nancy A. (2004). *Information Technology*

Auditing. Hoboken, New Jersey : John Wiley & Sons, Inc.

Institut Akuntan Publik Indonesia. (2001). Standar Profesional Akuntan Publik. Jakarta : Salemba Empat

Keputusan Presiden No. 80 tahun 2003 tentang Pedoman Pelaksanaan Pengadaan Barang / Jasa Pemerintah (Pedoman Pengadaan Barang / Jasa).

KPPU. (2009). Pedoman Pasal 22 tentang Larangan Persekongkolan dalam Tender Komisi Pengawas Persaingan Usaha. http://www.kppu.go.id/ baru/ index.php?aid=368&mode=art&mnid=65&encodurl=03%2F10%2F10%2C06%3A03%3A27. (Diakses pada 29 Januari 2010)

Tuanakotta, Theodorus M. (2007). Akuntansi Forensik dan Audit Investigatif. Jakarta: LPFEUI